AMENDMENTS TO THE CLAIMS

1. (Currently amended) A computer-implementable method for determining the behavior of an executable comprising:

[[(a)]] selecting evaluation calls made by the executable to the interface of an operating system;

[[(b)]] loading stubs into a virtual address space, the stubs:

[[(i)]] mirroring the calls made to the interface of an operating system wherein mirroring the calls made to the interface of the operating system includes mirroring a set of full implemented DLLs; and

[[(ii)]] determining a behavior signature for the selected calls;

wherein the calls are included in dynamic link libraries (DLLs) and wherein loading stubs include loading stub DLLs into said virtual address space;

[[(c)]] executing the selected calls inside of a virtual operating environment using the loaded stubs dynamically linked libraries; and

[[(d)]] determining the behavior signatures resulting from said execution of the selected calls inside of a virtual operating environment.

2. (Original) The method of Claim 1 wherein the calls selected for evaluation are a subset of calls made by the executable to the interface of an operating system.

3. (Original) The method of Claim 1 wherein the calls are application programming interface (API) calls.

4-5. (Canceled)

6. (Original) The method as recited in Claim 1 further comprising writing the behavior signature of the selected calls to an output store.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

7. (Currently amended) The method as recited in Claim 6 wherein writing the behavior signature to an output media includes writing three parameters to the output media comprising:

[[(a)]] a first parameter indicative of the call made to the operating system;

[[(b)]] a second parameter operative to store a variable of known data types; and

[[(c)]] a third parameter operative to store a variable of known data types.

8. (Currently amended) The method as recited in Claim 2, wherein selecting a subset of calls includes:

[[(a)]] traversing the executable's machine code and identifying calls that are directed to the interface of the operating system; and

[[(b)]] identifying calls that are potentially indicative of malware.

9. (Original) The method as recited in Claim 8, wherein identifying calls that are potentially indicative of malware includes:

comparing calls made in the executable with calls that exist in known malware; and

if a call matches one that exists in known malware, determining that the call is potentially indicative of malware.

10. (Original) The method as recited in Claim 8, wherein identifying calls that are potentially indicative of malware includes:

comparing calls made in the executable with calls that are identified as a future security threat from malware; and

if a call matches one that is identified as a future security threat from malware, determining that the call is potentially indicative of malware.

11. (Original) The method as recited in Claim 2, wherein selecting a subset of calls includes determining if each call requires execution by a stub.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

12. (Original) The method as recited in Claim 1, wherein loading stubs is initiated by an event generated by the virtual operating environment.

13. (Original) The method as recited in Claim 1, wherein loading stubs is performed by a loader that copies the stubs from a storage media to a virtual address space.

14. (Original) The method as recited in Claim 1, wherein loading stubs includes determining the stubs that handle the selected calls.

15. (Currently amended) A computer-readable medium bearing computer-executable instructions which, when executed, carry out a method for determining the behavior of an executable comprising:

[[(a)]] selecting evaluation calls made by the executable to the interface of an operating system;

[[(b)]] loading stubs into a virtual address space, the stubs:

[[(i)]] mirroring the calls made to the interface of an operating system wherein mirroring the calls made to the interface of the operating system includes mirroring a set of full implemented DLLs; and

[[(ii)]] determining a behavior signature for the selected calls;

wherein the calls are included in dynamic link libraries (DLLs) and wherein loading stubs include loading stub DLLs into said virtual address space;

[[(c)]] executing the selected calls inside of a virtual operating environment using the loaded stubs dynamically linked libraries; and

[[(d)]] determining the behavior signatures resulting from said execution of the selected calls inside of a virtual operating environment.

16. (Original) The computer-readable medium of Claim 15 wherein the calls selected for evaluation are a subset of calls made by the executable to the interface of an operating system.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

17. (Original) The computer-readable medium of Claim 15 wherein the calls are application programming interface (API) calls.

18-19. (Canceled)

20. (Original) The computer-readable medium of Claim 15 further comprising writing the behavior signature of the selected calls to an output store.

21. (Currently amended) The computer-readable medium of Claim 20 wherein writing the behavior signature to an output media includes writing three parameters to the output media comprising:

[[(a)]] a first parameter indicative of the call made to the operating system;

[[(b)]] a second parameter operative to store a variable of known data types; and

[[(c)]] a third parameter operative to store a variable of known data types.

22. (Currently amended) The computer-readable medium of Claim 16, wherein selecting a subset of calls includes:

[[(a)]] traversing the executable's machine code and identifying calls that are directed to the interface of the operating system; and

[[(b)]] identifying calls that are potentially indicative of malware.

23. (Original) The computer-readable medium of Claim 22, wherein identifying calls that are potentially indicative of malware includes:

comparing calls made in the executable with calls that exist in known malware; and

if a call matches one that exists in known malware, determining that the call is potentially indicative of malware.

24. (Original) The computer-readable medium of Claim 22, wherein identifying calls that are potentially indicative of malware includes:

comparing calls made in the executable with calls that are identified as a future security threat from malware; and

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

if a call matches one that is identified as a future security threat from malware, determining that the call is potentially indicative of malware.

25. (Original) The computer-readable medium of Claim 16, wherein selecting a subset of calls includes determining if each call requires execution by a stub.

26. (Original) The computer-readable medium of Claim 15, wherein loading stubs is initiated by an event generated by the virtual operating environment.

27. (Original) The computer-readable medium of Claim 15, wherein loading stubs is performed by a loader that copies the stubs from a storage media to a virtual address space.

28. (Original) The computer-readable medium of Claim 15, wherein loading stubs includes determining the stubs that handle the selected calls.

29-35. (Canceled)

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100